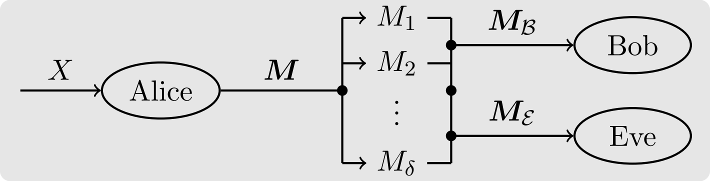
On the Computational Security of the Static Distributed Storage System

Annina Bracher, Eran Hof, and Amos Lapidoth

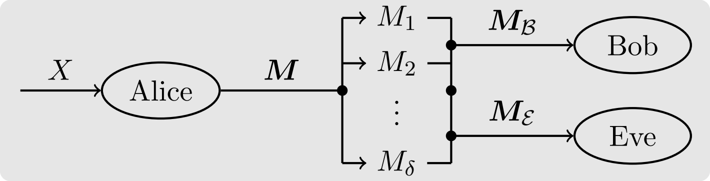
ETH Zürich, Switzerland

02.04.2015

Model

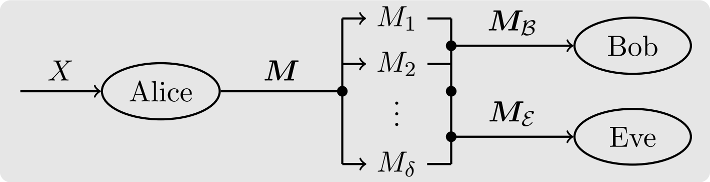

X
Alice
$\boldsymbol{M}$
M_1
M_2
$\vdots$
M_δ
$\boldsymbol{M}_{\mathcal{B}}$
$\boldsymbol{M}_{\mathcal{E}}$
Bob
Eve

Model



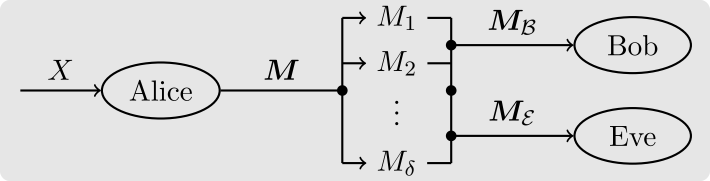
- $X \sim P_X$ is a password with finite support $\mathcal{X}$

Model



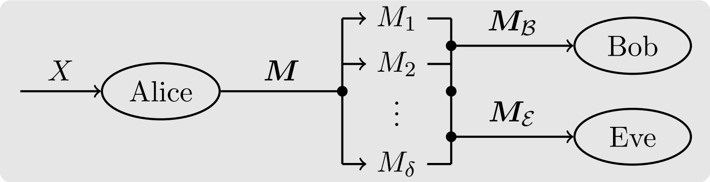
- $X \sim P_X$ is a password with finite support $\mathcal{X}$
- Alice describes X by δ s-bit hints $\boldsymbol{M} = (M_1, \dots, M_\delta) \in \mathbb{F}_{2^s}^\delta$

Model



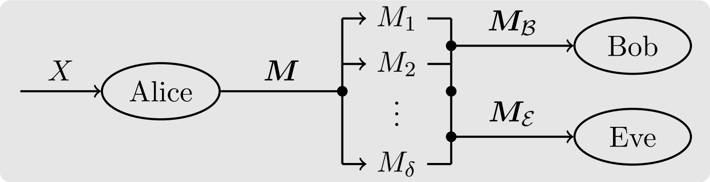
- $X \sim P_X$ is a password with finite support $\mathcal{X}$
- Alice describes X by δ s-bit hints $\boldsymbol{M} = (M_1, \ldots, M_\delta) \in \mathbb{F}_{2^s}^{\delta}$
- $M_1, \ldots, M_\delta$ are stored in different locations

Model



- $X \sim P_X$ is a password with finite support $\mathcal{X}$
- Alice describes X by δ s-bit hints $\boldsymbol{M} = (M_1, \ldots, M_\delta) \in \mathbb{F}_{2^s}^\delta$
- $M_1, \ldots, M_\delta$ are stored in different locations
- Robustness: Bob observes $\nu \leq \delta$ hints $\boldsymbol{M}_{\mathcal{B}}$, $\mathcal{B} \subseteq \{1, \ldots, \delta\}$
- Security: Eve observes $\eta < \nu$ hints $\boldsymbol{M}_{\mathcal{E}}$, $\mathcal{E} \subseteq \{1, \ldots, \delta\}$

Model



- $X \sim P_X$ is a password with finite support $\mathcal{X}$
- Alice describes X by δ s-bit hints $\boldsymbol{M} = (M_1, \ldots, M_\delta) \in \mathbb{F}_{2^s}^\delta$
- $M_1, \ldots, M_\delta$ are stored in different locations
- Robustness: Bob observes $\nu \leq \delta$ hints $\boldsymbol{M}_{\mathcal{B}}$, $\mathcal{B} \subseteq \{1, \ldots, \delta\}$
- Security: Eve observes $\eta < \nu$ hints $\boldsymbol{M}_{\mathcal{E}}$, $\mathcal{E} \subseteq \{1, \ldots, \delta\}$
- Bob and Eve want to access the account secured by X

Ambiguity

- Hopefully, Bob succeeds and Eve does not. Therefore:

Goal

Bob's ambiguity about X shall be small and Eve's large.

Ambiguity

- Hopefully, Bob succeeds and Eve does not. Therefore:

Goal

Bob's ambiguity about X shall be small and Eve's large.

We measure ambiguity by ...

1. ... the number of guesses that are necessary to find X
2. ... the size of the smallest list that contains X

Ambiguity

- Hopefully, Bob succeeds and Eve does not. Therefore:

Goal

Bob's ambiguity about X shall be small and Eve's large.

We measure ambiguity by ...

1. ... the number of guesses that are necessary to find X
2. ... the size of the smallest list that contains X

Two versions: guessing and list

	Bob	Eve
Guessing version	1	1
List version	2	1

Guesses and List-Size

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

Guesses and List-Size

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

---

Guessing Massey 1994, Arikan 1996

- $G(\cdot|y)\colon \mathcal{X} \to [1 : |\mathcal{X}|]$ is for all $y \in \mathcal{Y}$ one-to-one

Guesses and List-Size

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

Guessing Massey 1994, Arikan 1996

- $G(\cdot|y)\colon \mathcal{X} \to [1 : |\mathcal{X}|]$ is for all $y \in \mathcal{Y}$ one-to-one
- $G(\cdot|Y)$ is a guessing function:

  $G(x|y) = l$ $\Leftrightarrow$ "Is $X = x$?" is the ℓ-th guess given $Y = y$

Guesses and List-Size

$(X,Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

Guessing Massey 1994, Arikan 1996

- $G(\cdot|y)\colon \mathcal{X} \to [1:|\mathcal{X}|]$ is for all $y \in \mathcal{Y}$ one-to-one
- $G(\cdot|Y)$ is a guessing function:
  $\boxed{G(x|y) = l} \Leftrightarrow$ "Is $X = x$?" is the ℓ-th guess given $Y = y$
- The ambiguity about X is $\mathbb{E}[G(X|Y)^\rho]$

Guesses and List-Size

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

Guessing Massey 1994, Arikan 1996

- $G(\cdot|y)\colon \mathcal{X} \to [1 : |\mathcal{X}|]$ is for all $y \in \mathcal{Y}$ one-to-one
- $G(\cdot|Y)$ is a guessing function:
  $G(x|y) = l$ $\Leftrightarrow$ "Is $X = x$?" is the ℓ-th guess given $Y = y$
- The ambiguity about X is $\mathbb{E}[G(X|Y)^\rho]$

List-Decoding Bunte & Lapidoth 2014

- For all $y \in \mathcal{Y}$, define $\mathcal{L}_y \triangleq \{x \in \mathcal{X} \colon P_{X|Y}(x|y) > 0\}$

Guesses and List-Size

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

Guessing Massey 1994, Arikan 1996

- $G(\cdot|y)\colon \mathcal{X} \to [1 : |\mathcal{X}|]$ is for all $y \in \mathcal{Y}$ one-to-one
- $G(\cdot|Y)$ is a guessing function:
  $G(x|y) = l$ $\Leftrightarrow$ "Is $X = x$?" is the ℓ-th guess given $Y = y$
- The ambiguity about X is $\mathbb{E}[G(X|Y)^\rho]$

List-Decoding Bunte & Lapidoth 2014

- For all $y \in \mathcal{Y}$, define $\mathcal{L}_y \triangleq \{x \in \mathcal{X} \colon P_{X|Y}(x|y) > 0\}$
- $\mathcal{L}_y$ is the smallest list $\mathcal{L}$ such that $P_{X|Y}(\mathcal{L}|y) = 1$

Guesses and List-Size

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

Guessing Massey 1994, Arikan 1996

- $G(\cdot|y)\colon \mathcal{X} \to [1 : |\mathcal{X}|]$ is for all $y \in \mathcal{Y}$ one-to-one
- $G(\cdot|Y)$ is a guessing function:
  $G(x|y) = l$ $\Leftrightarrow$ "Is $X = x$?" is the ℓ-th guess given $Y = y$
- The ambiguity about X is $\mathbb{E}[G(X|Y)^\rho]$

List-Decoding Bunte & Lapidoth 2014

- For all $y \in \mathcal{Y}$, define $\mathcal{L}_y \triangleq \{x \in \mathcal{X}\colon P_{X|Y}(x|y) > 0\}$
- $\mathcal{L}_y$ is the smallest list $\mathcal{L}$ such that $P_{X|Y}(\mathcal{L}|y) = 1$
- The ambiguity about X is $\mathbb{E}[|\mathcal{L}_Y|^\rho]$

Ambiguity: the Definition

Bob's ambiguity

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_X) = \min_{G_{\mathcal{B}}} \mathbb{E}\left[\max_{\mathcal{B}} G_{\mathcal{B}}(X|\boldsymbol{M}_{\mathcal{B}})^{\rho}\right] \qquad \text{(Guessing Version)}$$

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_X) = \mathbb{E}\left[\max_{\mathcal{B}} |\mathcal{L}_{\boldsymbol{M}_{\mathcal{B}}}|^{\rho}\right] \qquad \text{(List Version)}$$

Eve's ambiguity

$$\mathscr{A}_{\mathrm{E}}(P_X) = \min_{G_{\mathcal{E}}} \mathbb{E}\left[\min_{\mathcal{E}} G_{\mathcal{E}}(X\,|\boldsymbol{M}_{\mathcal{E}}\,)^{\rho}\right]$$

- $\mathcal{B} \subseteq \{1, \ldots, \delta\}$ has size $\nu \leq \delta$
- $\mathcal{E} \subseteq \{1, \ldots, \delta\}$ has size $\eta < \nu$
- Worst-case: given X Bob observes the worst ν hints $\boldsymbol{M}_{\mathcal{B}}$ and Eve the best η hints $\boldsymbol{M}_{\mathcal{E}}$

Finite-Blocklength Results: Guessing Version

1. We can achieve $\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_X) \le \mathscr{U}_{\mathrm{B}}$ for

$$\mathscr{U}_{\mathrm{B}} \ge 1 + 2^{\rho(H_{\tilde{\rho}}(X) - \nu s + 1)},$$

$$\mathscr{A}_{\mathrm{E}}(P_X) \ge \frac{c_{\rho,\delta,\eta}}{(1+\ln|\mathcal{X}|)^{\rho}} \Big[\big(2^{\rho(\nu-\eta)s} (\mathscr{U}_{\mathrm{B}} - 1) \big) \wedge 2^{\rho H_{\tilde{\rho}}(X)} \Big].$$

2. Conversely, if $\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_X) \le \mathscr{U}_{\mathrm{B}}$ holds, then

$$\mathscr{U}_{\mathrm{B}} \ge \frac{2^{\rho(H_{\tilde{\rho}}(X) - \nu s)}}{(1+\ln|\mathcal{X}|)^{\rho}} \vee 1,$$

$$\mathscr{A}_{\mathrm{E}}(P_X) \le 2^{\rho(\nu-\eta)s} \mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_X) \wedge 2^{\rho H_{\tilde{\rho}}(X)}.$$

$H_{\tilde{\rho}}(X) = \frac{1}{\rho} \log \Big(\sum_{x \in \mathcal{X}} P_X(x)^{\tilde{\rho}} \Big)^{\frac{1}{\tilde{\rho}}}$ is the Rényi entropy of order $\tilde{\rho} = \frac{1}{1+\rho}$

Finite-Blocklength Results: List Version

1. We can achieve $\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_X) \leq \mathscr{U}_{\mathrm{B}}$ for

$$\mathscr{U}_{\mathrm{B}} \geq 1 + 2^{\rho(H_{\tilde{\rho}}(X) - \log(2^{\nu s} - \log|\mathcal{X}| - 2) + 2)},$$

$$\mathscr{A}_{\mathrm{E}}(P_X) \geq \frac{c_{\rho,\delta,\eta}}{(1 + \ln|\mathcal{X}|)^{\rho}} \Big[\big(2^{\rho(\nu-\eta)s}(\mathscr{U}_{\mathrm{B}} - 1)\big) \wedge 2^{\rho H_{\tilde{\rho}}(X)} \Big].$$

2. Conversely, if $\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_X) \leq \mathscr{U}_{\mathrm{B}}$ holds, then

$$\mathscr{U}_{\mathrm{B}} \geq 2^{\rho(H_{\tilde{\rho}}(X) - \nu s)} \vee 1,$$

$$\mathscr{A}_{\mathrm{E}}(P_X) \leq 2^{\rho(\nu-\eta)s} \mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_X) \wedge 2^{\rho H_{\tilde{\rho}}(X)}.$$

$H_{\tilde{\rho}}(X) = \frac{1}{\rho} \log\Big(\sum_{x \in \mathcal{X}} P_X(x)^{\tilde{\rho}}\Big)^{\frac{1}{\tilde{\rho}}}$ is the Rényi entropy of order $\tilde{\rho} = \frac{1}{1+\rho}$

Guessing and List-Decoding

A link between guessing and list-decoding

Let $(X, Y) \sim P_{X,Y}$ take value in a finite set $\mathcal{X} \times \mathcal{Y}$.

1. $\mathbb{E}[G^*(X|Y)^\rho] \leq \mathbb{E}[|\mathcal{L}_Y|^\rho]$
2. $\mathbb{E}[|\mathcal{L}_{Y,Z}|^\rho] \leq \mathbb{E}[G^*(X|Y)^\rho]$ holds for $Z = \lfloor \log G^*(X|Y) \rfloor$

Guessing and List-Decoding

A link between guessing and list-decoding

Let $(X, Y) \sim P_{X,Y}$ take value in a finite set $\mathcal{X} \times \mathcal{Y}$.

1. $\mathbb{E}[G^*(X|Y)^\rho] \leq \mathbb{E}[|\mathcal{L}_Y|^\rho]$
2. $\mathbb{E}[|\mathcal{L}_{Y,Z}|^\rho] \leq \mathbb{E}[G^*(X|Y)^\rho]$ holds for $Z = \lfloor \log G^*(X|Y) \rfloor$

Proof:

1. $x \in \mathcal{L}_y \Rightarrow G^*(x|y) \leq |\mathcal{L}_y|$
   $x \notin \mathcal{L}_y \Rightarrow P_{X|Y}(x|y) = 0$
2. $x \in \mathcal{L}_{y,z} \Rightarrow |\mathcal{L}_{y,z}| \leq 2^{\lfloor \log G^*(x|y) \rfloor} \leq G^*(x|y)$

Guessing and List-Decoding

A link between guessing and list-decoding

Let $(X, Y) \sim P_{X,Y}$ take value in a finite set $\mathcal{X} \times \mathcal{Y}$.

1. $\mathbb{E}[G^*(X|Y)^\rho] \leq \mathbb{E}[|\mathcal{L}_Y|^\rho]$
2. $\mathbb{E}[|\mathcal{L}_{Y,Z}|^\rho] \leq \mathbb{E}[G^*(X|Y)^\rho]$ holds for $Z = \lfloor \log G^*(X|Y) \rfloor$

Proof:

1. $x \in \mathcal{L}_y \Rightarrow G^*(x|y) \leq |\mathcal{L}_y|$
   $x \notin \mathcal{L}_y \Rightarrow P_{X|Y}(x|y) = 0$
2. $x \in \mathcal{L}_{y,z} \Rightarrow |\mathcal{L}_{y,z}| \leq 2^{\lfloor \log G^*(x|y) \rfloor} \leq G^*(x|y)$

Remarks:

- $|\mathcal{Z}| \leq 1 + \log |\mathcal{X}|$
- $\frac{|\mathcal{Z}|^{-\rho} 2^{\rho H_{\tilde{\rho}}(X|Y)}}{(1+\ln|\mathcal{X}|)^{-\rho}} \leq \mathbb{E}[G^*(X|Y,Z)^\rho] \leq 2^{\rho H_{\tilde{\rho}}(X|Y)}$

Asymptotic Results

- $X = X^n$ is an n-tuple produced by the source $\{X_i\}$
- The Rényi entropy-rate $H_{\tilde{\rho}}(\boldsymbol{X}) = \lim_{n\to\infty} H_{\tilde{\rho}}(X^n)/n$ exists
- $s = nR_s$, where $R_s > 0$ is the per-hint storage-rate

Asymptotic Results

- $X = X^n$ is an n-tuple produced by the source $\{X_i\}$
- The Rényi entropy-rate $H_{\tilde{\rho}}(\boldsymbol{X}) = \lim_{n\to\infty} H_{\tilde{\rho}}(X^n)/n$ exists
- $s = nR_s$, where $R_s > 0$ is the per-hint storage-rate
- Achievable ambiguity exponent: $E_{\mathrm{E}} \geq 0$ such that

$$\lim_{n\to\infty} \mathscr{A}_{\mathrm{B}}(P_{X^n}) = 1, \quad \liminf_{n\to\infty} \frac{\log(\mathscr{A}_{\mathrm{E}}(P_{X^n}))}{n} \geq E_{\mathrm{E}}$$

hold for some sequence of stochastic encoders

Asymptotic Results

- $X = X^n$ is an n-tuple produced by the source $\{X_i\}$
- The Rényi entropy-rate $H_{\tilde{\rho}}(\boldsymbol{X}) = \lim_{n\to\infty} H_{\tilde{\rho}}(X^n)/n$ exists
- $s = nR_s$, where $R_s > 0$ is the per-hint storage-rate
- Achievable ambiguity exponent: $E_{\mathrm{E}} \geq 0$ such that

$$\lim_{n\to\infty} \mathscr{A}_{\mathrm{B}}(P_{X^n}) = 1, \quad \liminf_{n\to\infty} \frac{\log(\mathscr{A}_{\mathrm{E}}(P_{X^n}))}{n} \geq E_{\mathrm{E}}$$

  hold for some sequence of stochastic encoders
- Privacy-exponent: $\overline{E_{\mathrm{E}}} \triangleq \sup E_{\mathrm{E}}$ (possibly $-\infty$)

Asymptotic Results

- $X = X^n$ is an n-tuple produced by the source $\{X_i\}$
- The Rényi entropy-rate $H_{\tilde{\rho}}(\boldsymbol{X}) = \lim_{n\to\infty} H_{\tilde{\rho}}(X^n)/n$ exists
- $s = nR_s$, where $R_s > 0$ is the per-hint storage-rate
- Achievable ambiguity exponent: $E_{\mathrm{E}} \geq 0$ such that

$$\lim_{n\to\infty} \mathscr{A}_{\mathrm{B}}(P_{X^n}) = 1, \quad \liminf_{n\to\infty} \frac{\log(\mathscr{A}_{\mathrm{E}}(P_{X^n}))}{n} \geq E_{\mathrm{E}}$$

  hold for some sequence of stochastic encoders
- Privacy-exponent: $\overline{E_{\mathrm{E}}} \triangleq \sup E_{\mathrm{E}}$ (possibly $-\infty$)

$$\overline{E_{\mathrm{E}}} = \begin{cases} \rho\big(R_s(\nu - \eta) \wedge H_{\tilde{\rho}}(\boldsymbol{X})\big), & \nu R_s > H_{\tilde{\rho}}(\boldsymbol{X}) \\ -\infty, & \nu R_s < H_{\tilde{\rho}}(\boldsymbol{X}). \end{cases}$$

Optimal Guessing

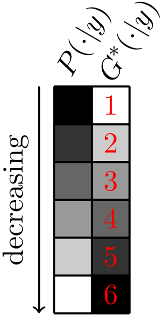
$(X,Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

What is $\min_G \mathbb{E}[G(X|Y)^\rho] = \mathbb{E}[G^*(X|Y)^\rho]$?

Optimal Guessing

$(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

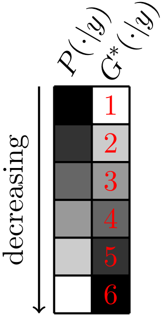
What is $\min_G \mathbb{E}[G(X|Y)^\rho] = \mathbb{E}[G^*(X|Y)^\rho]$?



Optimal Guessing

$(X,Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$, and $\rho > 0$ is fixed

What is $\min_G \mathbb{E}[G(X|Y)^\rho] = \mathbb{E}[G^*(X|Y)^\rho]$?



Optimal guessing Arikan 1996

$$\frac{2^{\rho H_{\tilde\rho}(X|Y)}}{(1+\ln|\mathcal{X}|)^{-\rho}} \vee 1 \le \mathbb{E}[G^*(X|Y)^\rho] \le 2^{\rho H_{\tilde\rho}(X|Y)}.$$

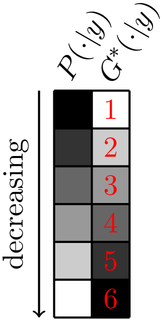
$H_{\tilde\rho}(X|Y) = \frac{1}{\rho}\log \sum_{y\in\mathcal{Y}} \Big(\sum_{x\in\mathcal{X}} P_{X,Y}(x,y)^{\tilde\rho}\Big)^{\frac{1}{\tilde\rho}}$ is Arimoto's conditional Rényi entropy of order $\tilde\rho = \frac{1}{1+\rho}$

Benefit of Additional SI

- $(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$
- Given the support $\mathcal{Z}$ of Z, we choose $P_{Z|X,Y}$

Benefit of Additional SI

- $(X, Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$
- Given the support $\mathcal{Z}$ of Z, we choose $P_{Z|X,Y}$



Q: What is $\min_{G, P_{Z|X,Y}} \mathbb{E}[G(X|Y,Z)^\rho]$?

Benefit of Additional SI

- $(X,Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$
- Given the support $\mathcal{Z}$ of Z, we choose $P_{Z|X,Y}$

decreasing

$P(\cdot\|y)$	$G^*(\cdot\|y)$	$z(\cdot,y)$	$G^*(\cdot\|y,z)$
	1	$\star$	1
	2	$\bullet$	1
	3	$\diamond$	1
	4	$\star$	2
	5	$\bullet$	2
	6	$\diamond$	2

$\mathcal{Z} = \{\ \star, \bullet, \diamond\ \}$

Q: What is $\min_{G, P_{Z|X,Y}} \mathbb{E}[G(X|Y,Z)^\rho]$?

For an optimal $P_{Z|X,Y}$ ...

- ... $Z = z(X,Y)$
- ... $G(x|y, z(x,y)) = \lceil G^*(x|y)/|\mathcal{Z}| \rceil$

Benefit of Additional SI

- $(X,Y) \sim P_{X,Y}$ takes value in a finite set $\mathcal{X} \times \mathcal{Y}$
- Given the support $\mathcal{Z}$ of Z, we choose $P_{Z|X,Y}$

decreasing

$P(\cdot\|y)$	$G^*(\cdot\|y)$	$z(\cdot,y)$	$G^*(\cdot\|y,z)$
	1	$\star$	1
	2	$\bullet$	1
	3	$\diamond$	1
	4	$\star$	2
	5	$\bullet$	2
	6	$\diamond$	2

$\mathcal{Z} = \{\star, \bullet, \diamond\}$

Q: What is $\min_{G, P_{Z|X,Y}} \mathbb{E}[G(X|Y,Z)^\rho]$?

For an optimal $P_{Z|X,Y}$ ...

- ... $Z = z(X,Y)$
- ... $G(x|y, z(x,y)) = \lceil G^*(x|y)/|\mathcal{Z}| \rceil$

A: $\mathbb{E}[\lceil G^*(X|Y)/|\mathcal{Z}| \rceil^\rho]$

Proof of the Results

The Result in a Nutshell

An ambiguity pair $\big(\mathscr{A}_{\mathrm{B}}(P_X), \mathscr{A}_{\mathrm{E}}(P_X)\big)$ is achievable iff
$\mathscr{A}_{\mathrm{B}}(P_X) \gtrsim 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)} \vee 1$
$\mathscr{A}_{\mathrm{E}}(P_X) \lesssim 2^{\rho(\nu-\eta)s} \mathscr{A}_{\mathrm{B}}(P_X) \wedge 2^{\rho H_{\tilde{\rho}}(X)}$.

- The converse holds by the results on optimal guessing

Proof of the Results

The Result in a Nutshell

An ambiguity pair $\left(\mathscr{A}_{\mathrm{B}}(P_X), \mathscr{A}_{\mathrm{E}}(P_X)\right)$ is achievable iff
$\mathscr{A}_{\mathrm{B}}(P_X) \gtrsim 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)} \vee 1$
$\mathscr{A}_{\mathrm{E}}(P_X) \lesssim 2^{\rho(\nu-\eta)s} \mathscr{A}_{\mathrm{B}}(P_X) \wedge 2^{\rho H_{\tilde{\rho}}(X)}$.

- The converse holds by the results on optimal guessing
- Achievability can be proved using nested MDS codes

Proof of the Results: Achievability

Insecure Encoding:

- Describe X by $V \in \mathbb{F}_{2^s}^{\nu}$ s.t. $\mathbb{E}[G(X|V)^{\rho}] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- Alice encodes V using a (δ, ν) MDS code
- She stores each codeword-symbol on a different hint

Proof of the Results: Achievability

Insecure Encoding:

- Describe X by $V \in \mathbb{F}_{2^s}^{\nu}$ s.t. $\mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- Alice encodes V using a (δ, ν) MDS code
- She stores each codeword-symbol on a different hint
- $\mathscr{A}_{\mathrm{B}}(P_X) = \mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- $\mathscr{A}_{\mathrm{E}}(P_X) \gtrsim 2^{\rho(H_{\tilde{\rho}}(X)-\eta s)} \approx 2^{\rho(\nu-\eta)s} \mathscr{A}_{\mathrm{B}}(P_X)$

Proof of the Results: Achievability

Insecure Encoding:

- Describe X by $V \in \mathbb{F}_{2^s}^{\nu}$ s.t. $\mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- Alice encodes V using a (δ, ν) MDS code
- She stores each codeword-symbol on a different hint
- $\mathscr{A}_{\mathrm{B}}(P_X) = \mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- $\mathscr{A}_{\mathrm{E}}(P_X) \gtrsim 2^{\rho(H_{\tilde{\rho}}(X)-\eta s)} \approx 2^{\rho(\nu-\eta)s} \mathscr{A}_{\mathrm{B}}(P_X)$

Secure Encoding:

- Describe X by $W \in \mathbb{F}_{2^s}^{\nu-\eta}$ s.t. $\mathbb{E}[G(X|W)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-(\nu-\eta)s)}$
- Generate $U \sim \mathrm{Unif}(\mathbb{F}_{2^s}^{\eta})$ independently of X
- Alice encodes (U, W) using a nested (δ, ν) MDS code
- She stores each codeword-symbol on a different hint

Proof of the Results: Achievability

Insecure Encoding:

- Describe X by $V \in \mathbb{F}_{2^s}^{\nu}$ s.t. $\mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- Alice encodes V using a (δ, ν) MDS code
- She stores each codeword-symbol on a different hint
- $\mathscr{A}_{\mathrm{B}}(P_X) = \mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- $\mathscr{A}_{\mathrm{E}}(P_X) \gtrsim 2^{\rho(H_{\tilde{\rho}}(X)-\eta s)} \approx 2^{\rho(\nu-\eta)s}\mathscr{A}_{\mathrm{B}}(P_X)$

Secure Encoding:

- Describe X by $W \in \mathbb{F}_{2^s}^{\nu-\eta}$ s.t. $\mathbb{E}[G(X|W)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-(\nu-\eta)s)}$
- Generate $U \sim \mathrm{Unif}(\mathbb{F}_{2^s}^{\eta})$ independently of X
- Alice encodes (U, W) using a nested (δ, ν) MDS code
- She stores each codeword-symbol on a different hint
- $\mathscr{A}_{\mathrm{B}}(P_X) = \mathbb{E}[G(X|U,W)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-(\nu-\eta)s)}$
- $\mathscr{A}_{\mathrm{E}}(P_X) \approx 2^{\rho H_{\tilde{\rho}}(X)} \approx 2^{\rho(\nu-\eta)s}\mathscr{A}_{\mathrm{B}}(P_X)$

Proof of the Results: Achievability

Insecure Encoding:

- Describe X by $V \in \mathbb{F}_{2^s}^{\nu}$ s.t. $\mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- Alice encodes V using a (δ, ν) MDS code
- She stores each codeword-symbol on a different hint
- $\mathscr{A}_\mathrm{B}(P_X) = \mathbb{E}[G(X|V)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-\nu s)}$
- $\mathscr{A}_\mathrm{E}(P_X) \gtrsim 2^{\rho(H_{\tilde{\rho}}(X)-\eta s)} \approx 2^{\rho(\nu-\eta)s} \mathscr{A}_\mathrm{B}(P_X)$

Secure Encoding:

- Describe X by $W \in \mathbb{F}_{2^s}^{\nu-\eta}$ s.t. $\mathbb{E}[G(X|W)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-(\nu-\eta)s)}$
- Generate $U \sim \mathrm{Unif}(\mathbb{F}_{2^s}^{\eta})$ independently of X
- Alice encodes (U, W) using a nested (δ, ν) MDS code
- She stores each codeword-symbol on a different hint
- $\mathscr{A}_\mathrm{B}(P_X) = \mathbb{E}[G(X|U, W)^\rho] \approx 2^{\rho(H_{\tilde{\rho}}(X)-(\nu-\eta)s)}$
- $\mathscr{A}_\mathrm{E}(P_X) \approx 2^{\rho H_{\tilde{\rho}}(X)} \approx 2^{\rho(\nu-\eta)s} \mathscr{A}_\mathrm{B}(P_X)$

To achieve any ambiguity-pair: $(V, W) \in \mathbb{F}_{2^p}^{\nu} \times \mathbb{F}_{2^r}^{\nu}$ s.t. $p + r = s$

Thank you